UGRADERT

Cyberangrep

En risiko for Norge?

KRIGSSKOLEN

Marius Andreas Bekkevang

Militære studier: ledelse og landmakt

Emne fordypning

Krigsskolen

2017

Antall ord: 8363

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Krig har eksistert så lenge det har eksistert samfunn med motstridende interesser, enten det har vært ressurser, religion eller landegrenser. Krigens natur forblir, ifølge Clausewitz, en konstant treenighet mellom hatet i befolkningen i samfunnet, sjansespillet som generalene skal beherske og den logiske begrunnelsen politikerne har for å gå til krig (Clausewitz, 2012, s. 44). Forskjellen på dagens og gårsdagens krig har med andre ord ikke bakgrunn i dens natur, men hva nasjonene i krig har å føre krig med. Teknologisk utvikling har ført til at det ikke lenger er hensiktsmessig å føre krig på store, åpne sletter slik det foregikk i Napoleons-krigene. I første verdenskrig så en resultatet av maskingeværet, og i andre verdenskrig så en hvordan fly og stridsvogner fullstendig forandret hvordan krigen utspiller seg. Selv om det er lenge siden stormaktene i verden var involvert i konflikter på hver sin side har det vokst frem et nytt domene for krigføring, nemlig cyberdomenet.

I løpet av de senere årene har samfunnene i verden, og spesielt den vestlige verden, koblet seg mer og mer opp mot nettverk og internett. Flere samfunnskritiske systemer benytter seg av nettverksbaserte løsninger både for drift og vedlikehold, og stadig flere mennesker har tilgang til internett. Antallet mennesker med tilgang til internett har steget fra 1024 millioner i 2005 til 3488 millioner i 2016 (International Telecommunication Union, 2017), og sannsynligvis er dette en utvikling som kommer til å fortsette. Det at samfunnet generelt, og militære systemer, i stor grad benytter nettverksløsninger skaper både effektivitet og sårbarhet. NATO erklærte i 2014 at et cyberangrep mot et medlemsland ville kunne utløse Artikkel 5 på lik linje med andre angrep, gitt at skadeomfanget er tilsvarende (NATO, 2014, s. 72). Videre anerkjente NATO i 2016 Cyberspace som et operasjonsdomene på lik linje med land, sjø og luft (NATO, 2016, s. 70).

Informasjons- og kommunikasjonsteknologi (IKT) er med på å effektivisere hvordan både kommersiell og statlige systemer styres, ofte ved at installasjoner og prosesser kan fjernstyres og sentraliseres. Norge er et av landene i verden som benytter seg av IKT i størst grad, både innen privat næringsliv og for å styre ressurser og fasiliteter som samfunnet avhenger av (Norges offentlige utredninger, 2015, s. 15). Det er absolutt fordeler med å effektivisere ved hjelp av teknologiske løsninger, men på den annen side vil desto større del av

samfunnskritiske ressurser være sårbare for digitale angrep. Denne oppgaven søker å finne svaret på hva en må forvente å kunne forsvare seg mot i cyberdomenet.

1.2 Problemstilling

Alle mennesker i Norge i dag benytter seg av noe som er koblet til et nettverk, enten det er internett, intranett, fasttelefon eller TV. Likevel er det overraskende få mennesker som tenker over de potensielle sårbarhetene de står overfor dersom det nettverket de benytter seg av skulle rammes av et angrep, spesielt kommunikasjonsnettverk. Det er vanlig å ha diverse personlig informasjon lagret på mobiltelefon eller datamaskin, som igjen er knyttet til internett. I 2013 var det 5,9 millioner mobilabonnement i Norge, noe som er flere abonnement enn det er befolkning i landet (Gustavsen, 2015, s. 52). Formålet med denne oppgaven vil være å belyse en sårbarhet i samfunnet som mange ikke tenker over, nemlig vår avhengighet av IKT. Det er slik at feiltrinn på lavt nivå kan få store konsekvenser på et høyere nivå når alt av utstyr er koblet opp imot hverandre. Derfor er det viktig at den enkelte er klar over hva en risikerer når en benytter seg av sine eller arbeidsplassens elektroniske enheter. Med bakgrunn i dette har jeg valgt å undersøke følgende problemstilling:

Er det en risiko for at Norge skal bli utsatt for et cyberangrep som får konsekvenser for landets sikkerhet?

1.3 Avgrensninger

Cyberdomenet er enormt, og det er nødvendig å avgrense oppgavens omfang. Oppgaven vil ta for seg det som kan anses som Forsvarets ansvar innen cyberdomenet, hvilket vil si angrep i større skala. Det som skal til for at landets sikkerhet skal være truet er at kritiske samfunnsfunksjoner eller infrastruktur settes ut av spill, eller ved at samfunnskritisk informasjon hentes av ondsinnede aktører (Norges offentlige utredninger, 2015, s. 252). Kritiske samfunnsressurser er kraftforsyningen, vegtrafikken, jernbanetrafikken, kystfarten, luftfarten, sentral kriseledelse og krisehåndtering, vannforsyningen, bank- og finansvirksomheten, helse og omsorg, nødsentralene og nødnettet (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 3). Skillet mellom statlige og ikke-statlige aktører kan være vanskelig å trekke i cyberspace, men det er likevel viktig å kunne differensiere, både med tanke på respons og hvilken instans som er ansvarlig for denne. Det er Norge som er

sentralt i denne oppgaven, men andre sammenlignbare land vil kunne benyttes som eksempler. Hjørnesteinen i norsk sikkerhetspolitikk er NATO (Forsvarsdepartementet, 2012, s. 7), og oppgaven tar derfor noe for seg hvordan NATO og andre medlemmer av NATO behandler trusler i cyberdomenet.

1.4 Begrepsavklaring

Som nevnt tidligere er cyberforsvar noe den allmenne befolkning har lite innsikt i, og det vil derfor være nødvendig med noen begrepsavklaringer.

Cyberdomenet er alt som benyttes for å koble sammen, sende, lagre og produsere data. Det omfatter og det noe mer abstrakte, nemlig hele nettverket av sammenkoblede enheter. I sum er det både det fysiske utstyret og infrastruktur som benyttes, samt selve det digitale rommet de logiske koblingene finner sted (Gustavsen, 2015, s. 17).

Cyber er et prefiks som viser at ordet det benyttes sammen med henviser til noe i cyberdomenet (Forsvarsdepartementet, 2014, s. 5).

EKOM står for elektronisk kommunikasjon, og når det er flere enheter i et nettverk blir dette et EKOM-nett som er definert i Ekomloven:

> System for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår, herunder nettverkselementer som ikke er aktive. (Samferdselsdepartementet, 2003, §1-5)

Norske styresmakter benyttes som samlebetegnelse for Storting, regjering og kommisjoner tilhørende disse.

2 Metode

2.1 Valg av metode

Det er problemstillingen som vil gi rammer for hvilken metode en kan benytte seg av (Johannesen, Tufte, & Christoffersen, 2010, s. 99). Cybersikkerhet vokste frem som fagfelt så sent som på 1990-tallet, og det ble spådd om cyberkrigføring så tidlig som i 1993 (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 230). Det er til dags dato kun få hendelser der cyberdomenet har blitt utnyttet for å skape en taktisk eller strategisk mulighet eller fordel, hvilket betyr at rammene for å analysere sårbarheter og muligheter innen cyberdomenet ikke er fastsatt av faktiske hendelser. Hans-Inge Langø skisserer de tre akademiske hovedretningene innen debatten om cybersikkerhet, nemlig revolusjonistene, tradisjonalistene og økologene (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 238). Revolusjonistene har et syn på cyberdomenet som vektlegger de teoretiske mulighetene som foreligger, samtidig som de skisserer et domene som stadig utvikles og formes av organisasjoner, stater og enkeltpersoner på verdensbasis (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 231). På den andre siden av debatten finner vi tradisjonalistene, som argumenterer for at fraværet av omfattende cyberkrigføring er bevis for at det ikke er mulig i praksis (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 233). Økologene befinner seg i området mellom tradisjonalistene og revolusjonistene og disse beskriver gjerne cyberdomenet som et levende økosystem som formes av aktørene, og sammenligner cyberdomenet med land, sjø og luft. På denne måten vil økologene analysere muligheter der en sammenligner effekter med det som kan oppnås gjennom konvensjonell krigføring (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 236). Det er tradisjonalistene og revolusjonistene som i utgangspunktet danner rammene for analysen av problemstillingen i denne oppgaven.

Utgangspunktet for denne studien er en dokumentanalyse av relevante bøker, lover, retningslinjer, tekster og artikler for å finne svar på problemstillingen som nevnt tidligere. En dokumentanalyse tar for seg kvalitative data i tekstform, organiserer relevant data og analyserer og tolker dette opp mot problemstillingen (Johannesen, Tufte, & Christoffersen, 2010, s. 165). Oppgaven søker ikke å finne ut av hvordan Norge i dag opererer i cyberdomenet eller hvor ofte cyberhendelser finner sted. Med bakgrunn i dette og bachelorperiodens begrensede tidsramme ekskluderes intervju som innhentingsmetode. Flere

av dokumentene som analyseres har utgangspunkt i intervjuer med fagpersonell, samtidig som at det i utgangspunktet ikke er stor forskjell på om informasjonen en analyserer utarter seg i tekst eller lyd (Johannesen, Tufte, & Christoffersen, 2010, s. 164). Videre vil jeg trekke frem gjennomførte casestudier som kan benyttes som eksempler til sammenligning med norske forhold.

2.2 Anvendt metode

Innledningsvis var jeg interessert i å skrive en oppgave om hybrid krigføring, men innså tidlig at dette emnet ble for omfattende for bachelornivået. Undersøkelsene av materiale som omhandlet hybrid krigføring gjorde meg oppmerksom på det meget spennende feltet cyberkrigføring, som jeg undersøkte videre. Relevant teori innen cyberkrigføring har jeg primært funnet via søk i databasene biblioteket ved Krigsskolen abonnerer på, med søkeordene: *Cyber, cyber warfare, hybrid warfare og cyber defence.* Videre har jeg funnet relevante tidsskrifter, artikler og bøker i Krigsskolens bibliotekkatalog, samt at jeg har kunnet hente utredninger, stortingsproposisjoner og lovverk på regjeringen og Stortinget sine nettsider. Under Krigsskolens studietur til Brüssel i 2017 kom det frem at EU og NATO har rettet sitt søkelys mot cyberdomenet i stadig større grad de siste årene, noe som åpnet tilgangen på mer data for denne oppgaven.

For å besvare problemstillingen benyttet jeg sentral teori, analyser, reglement og rapporter som omhandlet cybersikkerhet som tema og innad i Norge. Med dette til grunn ble det klart hvilke typer angrep som er vanlige, og hvilket skadepotensiale som finnes i cyberangrep. Deretter benyttet jeg spesielt rapporter fra sikkerhetsmyndigheter i Norge for å se på hva som kan være mål i landet, og hvilke aktører som eventuelt kunne utgjøre en trussel. Det er i senere tid gjennomført analyser av sårbarheter i Norge, samt hva som eventuelt blitt resultatet av et omfattende cyberangrep. For å danne et helhetlig grunnlag for å besvare problemstillingen har jeg sett på både skadeomfanget av cyberangrep som er gjennomført i andre land, samt skadepotensialet sikkerhetsmyndighetene i Norge og NATO-land beskriver.

2.3 Kildevalg og kildekritikk

«Forskeren må være seg bevisst at han er en utvelgende aktør, og at data som brukes, ikke er uavhengige av hans forhåndsoppfatninger» (Johannesen, Tufte, & Christoffersen, 2010, s. 40). Dette er selvfølgelig tilfellet i denne oppgaven, selv om jeg har lite bakgrunnskunnskap om emnet fra før. Likevel er mitt syn nødvendigvis farget av at jeg er offiser i den norske hæren og således har jeg en vestlig tilnærming til verden generelt. For å holde meg så nøytral som mulig i forhold til problemstillingen har jeg basert meg på publikasjoner fra regjeringen, Stortinget, og i stor grad fagfellevurderte akademiske publikasjoner.

Med bakgrunn i sitatet «Kildekritikk handler om å vurdere en kildes troverdighet, objektivitet, nøytralitet og egnethet» (Enstad, 2016, s. 14) har jeg gjort et utvalg med fokus på de fire nevnte kriteriene. Kildene jeg har brukt er i stor grad fagfellevurderte, med unntak av publikasjonene fra norske styresmakter. Fagfellevurdering bidrar til å styrke tekstens troverdighet, da dette vil si at flere eksperter innenfor det gitte temaet vil si seg enig i at tekstens påstander er relevante og plausible (Enstad, 2016, s. 14). En svakhet som preger emnet cyberkrigføring og cybersikkerhet er at land som har kompetanse og erfaring innen både offensive og defensive operasjoner i cyberspace holder informasjon om dette strengt hemmelig. Hemmeligholdet har begynt å lette litt i senere tid, men de skarpeste kapasitetene holdes trolig hemmelige inntil de benyttes. Dersom en publiserer hvilke kapasiteter en besitter for cyberoperasjoner vil motstanderen en kan benytte gitte kapasiteter mot ha mulighet til å rette opp i sårbarheter og feil som lukker mulighetsvinduet fullstendig (Limnéll, 2015, s. 524).

Publikasjoner utgitt av styresmaktene i Norge vil nødvendigvis ha en agenda, enten det er å opplyse befolkningen, danne trygge retningslinjer i samfunnet, eller rett og slett å sørge for stemmer til gjenvalg. Disse er likevel sentrale for å besvare problemstillingen, da det er Norges retningslinjer for cybervirksomhet som vil være styrende for mulighetene andre aktører har til å gjennomføre cyberangrep mot Norge. Politiske publikasjoner holder ikke samme standard som akademiske tekster hva gjelder kildehenvisninger og argumentasjon, og disse må derfor tolkes for det de representerer.

3 Teori

3.1 Fremveksten av cyberdomenet

Det som i dag omtales som cyberdomenet kan spores tilbake til det som var et nettverk for at forskere skulle kunne utveksle informasjon som ble etablert av den militære forskningsinstitusjonen *Advanced Research Project Agency (ARPA)* i USA. Gjennom 1980-tallet vokste dette nettverket fram innen sivile og militære forskningsinstitusjoner. World Wide Web ble tilgjengelig fra 1993, som markerer starten på det vi i dag kjenner som internett. Siden den tid har utviklingen og tilgjengeligheten av dette verdensomspennende nettverket økt i enorm hastighet (Store Norske Leiksikon, 2017). Norge ble i 1972 det første landet utenom USA til å koble seg til ARPANET (Norges offentlige utredninger, 2015, s. 101). I løpet av de siste to tiårene har flere samfunnskritiske systemer blitt koblet opp mot internett for å forenkle og effektivisere drift. Denne typen prosesskontrollsystemer kalles *Supervisory Control And Data Aquisition (SCADA)* (Norges offentlige utredninger, 2015, s. 41). Flere av disse systemene er koblet opp mot internett med dårlig eller fraværende sikring, som gjør de svært utsatt for angrep (Rid, 2013, s. 68).

Internett og bruken av det er i kontinuerlig utvikling og endring, og det deles inn i tre generasjoner av internett, der *Web 1.0* var utbygging at infrastruktur og kommersialisering, *Web 2.0* innebar sosiale medier, og *Web 3.0* er dagens fase der mobile enheter tilknyttet internett smelter sammen den fysiske og virtuelle verden (Langø & Sandvik, Cyberspace og sikkerhet, 2013, s. 222). Når en stadig større del av samfunnskritiske ressurser og samfunnet for øvrig er koblet til internett danner dette grunnlaget for at aktører med ondsinnede hensikter kan angripe og utnytte en større gruppe mennesker. Forsvarsdepartementet definerer *cyberhendelse* til «(…) både om situasjoner der IKT-systemer blir utsatt for cyberangrep, og ved utilsiktet svikt forårsaket av ulykker eller uhell» (Forsvarsdepartementet, 2014, s. 21). Denne oppgaven vil nødvendigvis ikke ta for seg utilsiktede hendelser som uhell og hendelser forårsaket av naturlige fenomen som vær og skred. Denne typen hendelser kan likevel få tilsvarende konsekvenser, som i romjulen 2011 da orkanen *Dagmar* førte til store utfordringer i kriseledelse fordi den satte EKOM-tjenester ut av spill. Dette førte til at befolkningen som var rammet følte seg utrygg (Gustavsen, 2015, s. 13). Tilsiktede IKT-hendelser deles inn i IKT-kriminalitet, digitale angrep, spionasje, sabotasje og terror (Norges offentlige utredninger, 2015, s. 54). Som spennet av begrep antyder er det en stor mengde forskjellige aktører i cyberspace, som besitter varierende grad av ressurser, kunnskap og organisasjon

(Norges offentlige utredninger, 2015, s. 54). Etterretningstjenestens vurdering *Fokus 2017* fastsetter at det forventes økt aktivitet mot Norge, spesielt innen russisk og kinesisk cyberbasert etterretningsvirksomhet (Etterretningstjenesten, 2017, s. 34).

3.2 Cybertrusler og aktører

3.2.1 Cybertrusler

Som mange er klar over finnes det utallige muligheter for å trykke på feil link eller godta feil varsel og ende opp med en eller annen form for infeksjon av sin datamaskin. Når det er snakk om cybertrusler relevante for denne oppgaven kan spennet av kilder for sårbarheten som utnyttes gå fra ansatte i en bedrift som i uvitenhet installerer ondsinnet programvare til sårbarheter i komponenter og programmer i et system. *Cyberangrep* vil si «Handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et informasjonssystem» (Forsvarsdepartementet, 2014, s. 21). Som det kommer frem av definisjonen kan cyberangrep ramme flere sider av samfunnet, alt fra enkeltpersoner til integriteten av systemer. Likevel er det per i dag ikke så mange forskjellige metoder for å gjøre dette, og en forståelse for disse er nødvendig for videre diskusjon. Metodene som benyttes går langs et spektrum fra alminnelige ikke-målrettede angrep med lavt skadepotensiale til målrettede angrep med stort skadepotensiale (Rid, 2013, s. 36). Dette delkapitlet tar for seg tre typer cyberangrep som har blitt benyttet for å angripe kritiske samfunnsressurser i andre land, som fremkommer av eksemplene senere i kapitlet. Skadepotensiale og kompleksiteten i angrepsmetodene er listet i stigende rekkefølge, og disse er og de tre hovedtypene av cyberangrep som gjennomføres i dag (Langø & Sandvik, Cyberspace og sikkerhet, 2013, s. 224).

3.2.1.1 Denial of Service

Denial of Service (DoS) vil si at en aktør benytter seg av programvare for å belaste en funksjon eller nettside i så stor grad at andre brukere ikke vil få tilgang til å benytte seg av tjenesten eller nettsiden (Rid, 2013, s. 40). Dette er en type angrep som ikke krever veldig mye ressurser å gjennomføre, og det skaper heller ikke store skader for mottakeren annet enn eventuelt tap av omsetning og omdømme. Dersom aktøren på forhånd av angrepet har infisert

flere verter med koden kan det føre til større trafikk mot mottakeren av angrepet, og dette er kjent som et Distributed Denial of Service (DDoS) angrep. Denne typen angrep kan sette en nettside eller tjeneste ut av spill i alt fra minutter til noen dager, men fører ikke til fysisk skade på hverken personell eller materiell (Norges offentlige utredninger, 2015, s. 57).

3.2.1.2 Malware

Dette er en type programvare som kan variere ut ifra aktørens kunnskap og ressurser, alt fra enkle virus som brukeren av et system selv må godta å installere, til avanserte programmer som kan penetrere sikkerhetssystemer og selvstendig velge og påvirke programvare og prosesser (Rid, 2013, s. 39). Denne typen angrep kan vare til den blir oppdaget av systemet som er under angrep eller til den avslører seg selv. Slik programvare kan ha til hensikt å svekke omdømmet til de som er under angrep, eller det kan ha til hensikt å forstyrre prosesser over tid. Dersom det er å svekke omdømmet til en organisasjon eller et system vil programvaren avsløre seg selv, gjerne ved å skape en eller annen form for oppstyr, for eksempel ved å spille musikk som ved angrepet av *Atomic Energy Organization of Iran* (Rid, 2013, s. 33).

3.2.1.3 Zero-day vulnerability

Dette er en ukjent sårbarhet i et system som kan utnyttes av angripende aktører. Denne typen sårbarhet kan finnes i programvare, komponenter, eller standardinnstillinger, og vil repareres så snart den er kjent (Norges offentlige utredninger, 2015, s. 37). Dersom det er mange maskiner i nettverk kan det være nok at en av maskinene tilknyttet nettverket ikke har oppdatert sin programvare for at denne typen sårbarhet skal kunne utnyttes. Videre er det flere systemer som har denne typen sårbarheter som er kjent, men likevel ikke blir forbedret fordi det enten er for kostbart, eller fordi ny versjon av programvare ikke er kompatibel med systemene som er koblet inn (Regjeringen, 2012, s. 5).

3.2.2 Aktører

Det er en rekke aktører som utfører cyberangrep, men de kan stort sett deles inn i fire grupper; stater, kriminelle, aktivister (også kjent som hacktivister) og patriotiske hackere. Terrororganisasjoner ble forventet at skulle benytte seg av cyberangrep, men disse har kun

benyttet seg av cyberdomenet for å spre ideologi og rekruttering hittil (Langø & Sandvik, Cyberspace og sikkerhet, 2013, s. 225). Skillet mellom de forskjellige aktørene kommer best til syne ut ifra hvor sofistikert angrepet er, hvor mye ressurser som kreves, og hvilken type informasjon som eventuelt hentes ut fra systemet som er under angrep. Kriminelle aktører er ute etter økonomisk vinning, og retter seg ofte mot kredittkortinformasjon og annen informasjon som kan benyttes for å tjene penger (Langø & Sandvik, Cyberspace og sikkerhet, 2013, s. 225). Statlige aktører utvikler og benytter seg oftest av svært sofistikerte former for angrep og programvare, og kan på denne måten gjenkjennes, selv om det kan være tilnærmet umulig å bevise hvilken stat som står bak et angrep (Gustavsen, 2015, s. 61). Hacktivistene benytter seg av cyberangrep for å skape oppmerksomhet for sine kampsaker, og patriotiske hackere vil angripe fiender av nasjonalstaten de støtter. Det finnes eksempler på at hacktivister og patriotiske hackere er støttet av stater for å gjennomføre sine angrep (Langø & Sandvik, Cyberspace og sikkerhet, 2013, s. 225). Innen hver av de fire gruppene finnes det undergrupper, og det vil nødvendigvis være mange statlige aktører innen cybervirksomhet. I Norge har vi eksempelvis Cyberforsvaret, Nasjonal sikkerhetsmyndighet (NSM), Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Direktoratet for samfunnssikkerhet og beredskap (DSB) som alle opererer innen cyberdomenet i en eller annen form.

3.3 Cyberdomenets muligheter

Det er til enhver tid aktivitet i cyberspace, både normal aktivitet og en eller annen form for cyberangrep. Mye av denne aktiviteten både oppstår og rettes utenfor Norges virtuelle grenser, men likevel er det nok av hendelser for NSM å håndtere. I 2015 håndterte NSM Norwegian Computer Emergency Response Team (NorCERT) 20 886 saker, hvorav 22 var alvorlige dataangrep mot viktige virksomheter i offentlig eller privat sektor (Nasjonal sikkerhetsmyndighet, 2015, s. 17). Selv med dette antallet hendelser har vi i Norge ikke blitt utsatt for avanserte angrep med store konsekvenser. Teorien setter få grenser for det som er mulig i cyberdomenet, men det er ikke alt som er praktisk gjennomførbart. Den nevnte akademiske debatten som foregår rundt cyberkrigføring og cybersikkerhet omhandler nettopp dette, der revolusjonistene skisserer muligheter for katastrofale angrep på størrelse med et *Cyber Pearl Harbor* og tradisjonalistene mener dette ikke lar seg gjennomføre i virkeligheten (Langø, Den akademiske debatten om cybersikkerhet, 2013, s. 238). Det som er viktig når en skal se på mulighetene i cyberdomenet er at ingen av landene med størst kapasitet innen

cyberoperasjoner har stått ovenfor en eksistensiell trussel, og dermed neppe har benyttet seg av de mest voldelige og ødeleggende kapasitetene sine (Limnéll, 2015, s. 529). Skadepotensialet i cyberdomenet kan dermed antas å strekke seg utover det vi har sett i operasjoner som allerede er gjennomført, som vi skal se noen eksempler i dette delkapitlet.

3.3.1 Stuxnet

Stuxnet var en type malware-angrep rettet mot det iranske anlegget for anrikelse av uran i Natanz gjennomført som et samarbeid mellom USA og Israel (Rid, 2013, ss. 43, 45). For å gjennomføre dette angrepet måtte de som sto bak ha inngående kunnskap om programmering, industrielle kontrollsystemer og kjernefysikk. I tillegg til denne kunnskapen måtte de ha detaljert etterretning om anlegget de skulle angripe (Lindsay, 2013, s. 385). Deretter måtte koden lages og testes på tilsvarende materiell for å forvisse seg om at det ville være vellykket etter koden ble sendt mot sitt mål. Fasen for å samle etterretning og teste koden varte fra 2006 til koden infiserte anlegget i Natanz i 2009 (Lindsay, 2013, s. 387). I og med at anlegget i seg selv ikke var koblet til internett, men kun et internt nettverk, kjent som et *air gap* måtte koden først infisere industrielle selskaper som leverte komponenter eller programvare til anlegget i Natanz. Via uvitende teknikere fra disse selskapene ble nettverket som kontrollerte sentrifugene i anlegget infisert (Lindsay, 2013, s. 382). Straks koden var på plass i anlegget tok den kontroll over styringsenhetene til sentrifugene som anriket uran, samtidig som den viste normale verdier til skjermene til operatørene som overvåket anlegget. Deretter ville koden i sykluser på 27 dager skru opp tempoet til sentrifugen i 15 minutter for så å returnere til normal hastighet i 27 dager. Neste syklus ville den senke tempoet til sentrifugen i 50 minutter og returnere til normal hastighet i 27 dager. Slik fortsatte alle sentrifugene til de ble ødelagt på forskjellige tidspunkt (Lindsay, 2013, s. 384). Det at koden systematisk førte til at sentrifugene ble ødelagt sakte men sikkert i stedet for at samtlige ble ødelagt samtidig førte til at operatørene i anlegget ikke fattet mistanke. Koden ble ikke oppdaget før den førte til at en sivil datamaskin i Iran satt fast i en evig restart-syklus og et antivirusfirma ble kontaktet av eieren av maskinen (Lindsay, 2013, s. 365). Ødeleggelsene koden klarte å forårsake i tiden før den ble detektert viste seg å totalt sinke anrikningsprogrammet til Iran med et år (Lindsay, 2013, s. 390).

3.3.2 Ukraina

I mars 2014 entret russiske styrker Krim, noe som markerte starten på den fortsatt pågående konflikten i Øst-Ukraina (Limnéll, 2015, s. 527). I løpet av konflikten har det utspilt seg en rekke cyberhendelser uten at det nødvendigvis har blitt utpekt en skyldig aktør for samtlige hendelser. Det antas dog at angrepene er av russisk opphav. Nettsiden til ukrainske styresmakter ble angrepet og var ute av drift i 72 timer mens russiske styrker inntok Krim, og flere andre nettsider ble angrepet av DDoS-angrep. Samtidig ble flere parlamentsmedlemmers mobiltelefoner hacket (Limnéll, 2015, s. 528). Under presidentvalget i mai 2014 ble valgkommisjonens nettsider angrepet, og det ble publisert feilaktig informasjon om vinneren av valget, selv om selve valgresultatet ikke ble berørt. Russiske TV-kanaler publiserte umiddelbart historier om den påståtte vinneren av valget, noe som skapte usikkerhet i befolkningen (Limnéll, 2015, s. 528).

23. desember 2015 ble store deler av strømnettet i Ukraina rammet av et cyberangrep som førte til at 225,000 mennesker var uten strøm i en periode (E-ISAC SANS, 2016, s. iv). Dette angrepet hadde noen likhetstrekk med Stuxnet-angrepet ved at aktøren måtte ha god etterretning på hvilke komponenter systemet besto av, og hvordan disse ble kontrollert. Deretter ble systemene infisert med malware skrevet inn i Microsoft Office-dokumenter distribuert til ansatte i kraftverket. Når dette var gjort kunne angriperne ta kontroll over systemene når de selv mente tiden var inne. Trolig hadde de tilgang til systemet hele seks måneder før 23. desember (E-ISAC SANS, 2016, s. 6). Angriperne tok kontroll over systemet på flere forskjellige mellomstasjoner og stengte strømnettet synkronisert og effektivt slik at 225,000 mennesker forble uten strøm i flere timer (E-ISAC SANS, 2016, s. 2). Angrepet førte til at kraftselskapene måtte gå over til manuelle brytere for strømmen, og flere automatiske brytere ble ødelagt og måtte skiftes ut. Selv om angrepet ikke førte til strømstans i mer enn noen timer måtte kraftselskapet bruke flere måneder på reparasjoner og utskifting av berørte komponenter (Booz Allen Hamilton, 2016, s. 36).

3.3.3 Industrispionasjesaken i Telenor

I 2013 ble datamaskinene til flere sjefer i Telenor tappet for data, som ble oppdaget av Telenor Security Operations Centre (TSOC). Angrepet utartet seg ved at ledere i Telenor fikk tilsendt e-post fra kjente forbindelser som var skrevet på norsk og slik at alt så normalt ut (Gustavsen, 2015, s. 82). Vedlagt e-postene var filer eller linker til nettsider som installerte

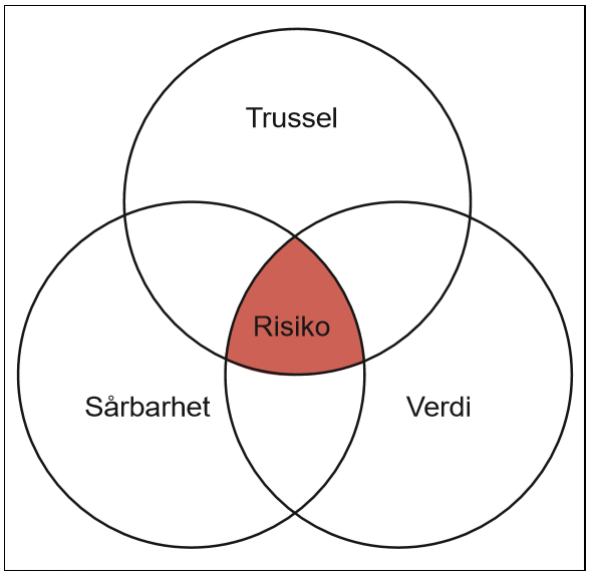
trojanske hester, en type programvare som ligger i bakgrunnen og videresender informasjon, på maskinen slik at passord, sensitiv informasjon, og de alle typer filer ble tappet fra maskinen (Gustavsen, 2015, s. 82). Et sikkerhetsselskap undersøkte den ondsinnede koden og fant ut at det var en del av et globalt nettverk av kommandoservere. Det stammet trolig fra India, og majoriteten av tilsvarende angrep var rettet mot pakistanske myndigheter og militære ledere. Det ble ikke funnet bevis for at angriperne var sponset eller under kommando av en nasjonalstat (Gustavsen, 2015, s. 83).

3.3.4 Oppsummering

Som de tre eksemplene tilsier er det et stort spenn i det som kan betraktes som cyberangrep. Stuxnet hadde som hensikt å forbli skjult og sabotere produksjonen av anriket uran over tid. Angrepene i Ukraina skapte mye forstyrrelser og usikkerhet samtidig som landet var og er i en væpnet konflikt. Disse angrepene skiller seg fra Stuxnet fordi de var mer intensive og kortvarige, altså skapte de større konsekvenser fort, og ble umiddelbart avdekket og håndtert. Industrispionasjesaken i Telenor hadde som hensikt å sanke informasjon fra ledere, men videre hensikt med dette angrepet er fortsatt ukjent. Når en skal diskutere sannsynligheten for cyberangrep er det viktig å forstå hensikten forskjellige aktører kan ha med å gjennomføre cyberoperasjoner, og disse eksemplene skal bidra til å øke denne forståelsen før videre diskusjon.

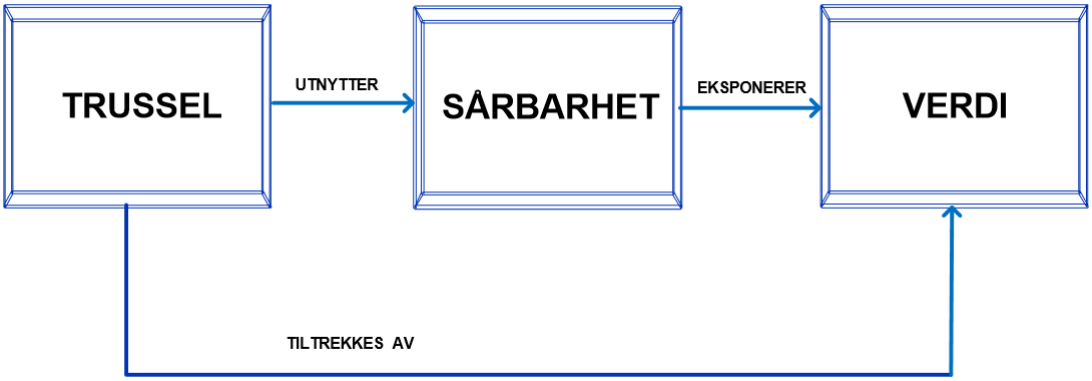
3.4 Risiko

Risiko er et sammensatt begrep som inneholder både et mål for sannsynlighet og konsekvens av at en uønsket hendelse finner sted (Norges offentlige utredninger, 2012, s. 68). For å beregne sannsynligheten og konsekvensen av at en aktør skulle gjennomføre en uønsket handling må en undersøke tre forhold, nemlig *verdi, sårbarhet* og *trussel* som vist i figur 1.



Figur 1: Samspillet mellom trussel, sårbarhet og verdi (Norges offentlige utredninger, 2012, s. 68)

Verdier er noe vi ønsker å beskytte, og kan bety alt fra liv og helse til fysiske objekter og infrastruktur, samt gradert informasjon (Norges offentlige utredninger, 2012, s. 68). I tillegg til disse verdiene er det en flere samfunnskritiske virksomheter hvis bortfall ville få store konsekvenser for hele samfunnet, enten direkte eller indirekte (Gustavsen, 2015, s. 18). Fordi verdiene er noe vi er avhengige av for at samfunnet skal fungere slik det vanligvis gjør, vil ondsinnede aktører tiltrekkes av å kunne påvirke Norge for å nå sine målsetninger. En aktør vil tiltrekkes av verdiene avhengig av verdiens egenskap og størrelse og hva aktøren kan oppnå av sine målsetninger ved å påvirke eller besitte disse (Mærli, 2012, s. 3). Trusselen en aktør utgjør baserer seg på hva aktøren vil oppnå, med hvilke midler, og hvilken hensikt (Mærli, 2012, s. 3). En trussel baserer seg derfor på at aktører har både vilje og evne til å gjennomføre et angrep for å nå sine mål. Sårbarheter kan forstås som en begrenset evne til å motstå påkjenninger som kan resultere i negative avvik fra normal funksjon (Norges offentlige utredninger, 2012, s. 68). Risiko oppstår derfor når en ondsinnet aktør ser en verdi han har evne og vilje til å angripe, aktøren utnytter en sårbarhet i beskyttelsen av denne verdien og oppnår sine målsetninger. Figur 2 viser denne kjeden som danner utgangspunktet for risiko.



Figur 2: Sammenhengen mellom verdi, trussel og sårbarhet (Mærli, 2012, s. 2).

Dette må ses i et overordnet samfunnsmessig perspektiv, men vil være sant på alle nivåer. Tyveri oppstår når tyven ser at noen har en verdi, eksempelvis en TV, og ønsker å stjele denne. Tyven vil da finne en sårbarhet å utnytte seg av for å få tilgang til TVen, for eksempel ved å knuse en rute eller åpne døren i huset. På den andre side vil personen som eier TVen ønske å beskytte sin verdi, og vil muligens investere i sterkere låser eller et alarmsystem. Dynamikken foregår på lik linje når det er snakk om verdier i samfunnet, selv om disse ikke er fysiske gjenstander i alle tilfeller (Norges offentlige utredninger, 2012, s. 68). Store verdier som ikke er beskyttet vil være enkle og effektive mål for aktører som ønsker å ramme Norge, mens mindre verdier kan være helt uinteressante selv om de ikke er beskyttet fordi aktørene ikke vil kunne nå sine mål ved å ramme verdien.

Når risiko skal vurderes knyttet til forhold som har med rikets sikkerhet å gjøre vil en ikke legge like stor vekt på sannsynlighet som på konsekvensen av en hendelse (Norges offentlige utredninger, 2006, s. 35). I disse tilfellene vil sårbarheter utbedres og defensive tiltak iverksettes for å verne om verdien, uavhengig av sannsynligheten for angrep eller hendelser (Norges offentlige utredninger, 2006, s. 35).

4 Drøfting

4.1 Verdifulle mål i Norge

Som nevnt er verdier noe vi ønsker å beskytte, og kan bety alt fra liv og helse til fysiske objekter og infrastruktur, gradert informasjon, og samfunnskritiske virksomheter hvis bortfall ville få store konsekvenser for hele samfunnet, enten direkte eller indirekte (Gustavsen, 2015, s. 18) (Norges offentlige utredninger, 2012, s. 68). Samfunnskritiske ressurser er kraftforsyningen, vegtrafikken, jernbanetrafikken, kystfarten, luftfarten, sentral kriseledelse og krisehåndtering, vannforsyningen, bank- og finansvirksomheten, helse og omsorg, nødsentralene og nødnettet (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 3). Det en må finne ut av er hvilke verdier som kan tenkes å være interessante for aktører innen cyberdomenet. Etterretningstjenestens rapport *Fokus 2017* peker mot at det primært er tre kategorier av digitale trusler vi står overfor, nemlig etterretning, sabotasje og påvirkning (Etterretningstjenesten, 2017, s. 36). En kan dedusere ut ifra dette at verdiene som er interessante er gradert informasjon, EKOM-infrastruktur/samfunnskritiske ressurser og folkets opinion. I tillegg til dette vil bedrifter og enkeltpersoner oppleve ikke-målrettede angrep fra kriminelle som søker å tjene penger.

Av de 22 alvorlige dataangrepene NSM håndterte i 2015 omhandlet de fleste spionasje mot viktige virksomheter i privat eller offentlig sektor (Nasjonal sikkerhetsmyndighet, 2015, s. 17). Når de fleste alvorlige dataangrep omhandler spionasje kan dette bety at målene som aktørene i cyberspace er interessert i kan være informasjon hentet ut av systemer, eller informasjon om selve systemene for fremtidige sabotasjeoperasjoner eller tilsvarende. Eksemplene fra Ukraina og Natanz viser begge at hensikten med angrepene var sabotasje, men likevel var systemene under angrep i flere måneder eller år for å hente etterretning om systemene (E-ISAC SANS, 2016, s. 6) (Lindsay, 2013, s. 387). Den andre faren med spionasjeoperasjoner er at dette kan benyttes i et konvensjonelt angrep mot Norge. Russland har en meget robust cyberkapasitet og har integrert cyberspionasje som del av en større strategi for å fremme deres globale interesser (Limnéll, 2015, s. 528). NSM fører tilsyn og kontroll over alle virksomheter som er omfattet av sikkerhetsloven, noe som per 2015 er over 600 virksomheter (Nasjonal sikkerhetsmyndighet, 2015, s. 10). Virksomhetene tilknyttet Forsvaret er åpenbare mål for cyberspionasje, mens virksomheter som understøtter samfunnet for øvrig kan være mål for sabotasjeoperasjoner, enten det er helsevesen, EKOM-leverandører

eller kraftleverandører. Dersom en potensiell fiende har informasjon om våre kapasiteter, operasjonsmønster, beredskapsplaner og tilsvarende vil det nødvendigvis utgjøre en strategisk fordel.

Enkeltpersoner og virksomheter i Norge blir stadig rammet av angrep fra kriminelle aktører, enten det er snakk om vinningskriminalitet eller industrispionasje. I en studie gjennomført av FN i 21 land svarer 1-17% av respondentene at de hadde vært utsatt for kriminalitet via internett, mens mindre enn 5% hadde vært utsatt for kriminalitet i den fysiske verden. I samme studie svarte 2-16% av bedrifter at de hadde vært utsatt for cyberkriminalitet (Norges offentlige utredninger, 2015, s. 55). Kriminelle handlinger på internett øker i tråd med samfunnets omfattende bruk av internett, hvilket er i ferd med å bli et reelt samfunnsproblem (Norges offentlige utredninger, 2015, s. 56). I Norge har så godt som alle banker opplevd enten direkte angrep eller at deres kunder har blitt utsatt for kriminelle angrep gjennom internett. Årlige økonomiske tap som følge av cyberkriminalitet er estimert til 20 milliarder kroner (Norges offentlige utredninger, 2015, s. 57).

4.1.1 Delkonklusjon

Verdiene i Norge som er interessante for aktører i cyberspace strekker seg helt fra enkeltpersoners bankinformasjon til beredskapsplaner på øverste politiske nivå. Det som er relevant for oppgavens problemstilling er det som omfatter samfunnskritiske ressurser, EKOM-infrastruktur og gradert informasjon om forsvar og beredskap. Som drøftingen over viser er det avdekket mange forsøk på spionasje mot bedrifter som er tilknyttet disse virksomhetene, og konklusjonen er derfor at det er verdiene som omfatter samfunnskritiske ressurser, EKOM-infrastruktur og informasjon om forsvar og beredskap som er aktuelle for aktører som kan utgjøre en trussel for Norge.

4.2 Aktører som utgjør en trussel mot Norge

Trussel innebærer hvilken vilje og evne aktører antas å inneha for å kunne gjennomføre uønskede handlinger for å nå sine mål (Norges offentlige utredninger, 2012, s. 68). I cyberspace finnes det som nevnt fire hovedkategorier aktører, og deres kompetansenivåer og ressurser varierer fra enkeltpersoner med en datamaskin og internettforbindelse til store organisasjoner med enorm prosessorkraft (Norges offentlige utredninger, 2015, s. 54). De

største nasjonale aktørene innen cyberspace er USA, Kina, Israel, Russland, Storbritannia, Tyskland, Frankrike og Iran (Wilson, 2016, s. 8). Det vil være naturlig å anta at medlemmer av NATO ikke vil være interessert i å gjennomføre noen form for angrep mot Norge. Israel har nær tilknytning til USA og andre NATO-land og kan heller ikke antas å være spesielt interessert i å gjennomføre cyberangrep mot Norge. De nasjonale aktørene som gjenstår er Kina, Russland og Iran. Kina og Russland er utpekt som aktører som vil trappe opp cyberangrep mot Norge som forsterker inntrykket av at disse kan utgjøre en trussel mot Norge (Etterretningstjenesten, 2017, s. 34).

Noe av det som gjør cyberdomenet lukrativt for alt fra kriminelle til statlige aktører er at det er vanskelig, og i noen tilfeller umulig, å bevise hvem som står bak angrep. I konvensjonelle angrep har det alltid vært mulig å vite hvem som sto bak angrepet, selv om det kom overraskende (Rid, 2013, s. 141). Dette er ikke tilfellet i cyberspace fordi det er mulig å benytte seg av tredjeparter for å maskere hvor angrepet stammer fra. Det er mulig å komme fram til den geografiske lokasjonen et angrep stammer fra, men det kan likevel være vanskelig å bevise hvorvidt en statlig aktør står bak (Clapper, 2016, s. 3). Økningen i statlig-sponsede cyberangrep kommer til dels som et resultat av at det hverken er stor sannsynlighet for å bli oppdaget og at det er et fravær av konsekvenser dersom det skjer (Limnéll, 2015, s. 525). Et av Forsvarets grunnleggende funksjoner i Norge er å ha en avskrekkende effekt på mulige angripere (Forsvarsdepartementet, 2016, s. 22). I cyberspace er det ikke mulig å oppnå en avskrekkende effekt på bakgrunn av det grunnleggende problemet en vil ha med å bevise hvilke aktører som står bak eventuelle angrep (Lindsay, 2013, s. 377).

Det at to av de største aktørene innen cybervirksomhet er utpekte aktører som gjennomfører operasjoner mot Norge er noe en må ta på alvor. Selv om Russland og Kina ikke har publiserte doktriner som beskriver deres cyberkapabiliteter, har begge land vist både vilje og evne til å benytte seg av cyberdomenet for offensive cyberoperasjoner både mot Norge og andre land (Wilson, 2016, s. 15) (Clapper, 2016, s. 3) (Limnéll, 2015, s. 525) (Etterretningstjenesten, 2017, s. 34). En tredje cyberstormakt som har vist evne og vilje til å gjennomføre offensive cyberoperasjoner er USA. Pentagon skisserte i 2015 muligheten for å benytte seg av *cyber fires* på følgende måter:

> Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes. (General Counsel of the Department of Defense, 2015, s. 1015)

Selv om dette er beskrivelse av hva som kan være eksempler på militære angrep i cyberspace og ikke nåværende kapasiteter har Laura Rojas, talskvinne for Pentagon, bekreftet at de jobber med å utvikle redskap og kapabiliteter for å kunne gjennomføre alle de tre nevnte angrepene (Sternstein, 2015, s. 2). Russland og Kina har ikke noen offentlige uttalelser, doktriner eller rapporter som beskriver hvilke kapasiteter de besitter innen cyberkrigføring, noe som gjør at en må anta at de utvikler sine kapasiteter med tilsvarende målsetninger som USA. Dersom vi da antar at Russland og Kina har tilsvarende evner innen cyberspace er deres vilje til å gjennomføre slike operasjoner mot Norge avgjørende. Antall alvorlige dataangrep som NSM har håndtert har gått fra 110 i 2014 til 22 i 2015 (Nasjonal sikkerhetsmyndighet, 2015, s. 17). Dette er en trend som ved første øyekast ser meget positiv ut, men sannheten er at det reelle antallet alvorlige angrep mot Norge neppe har sunket. Årsaken til at færre angrep håndteres er at kompleksiteten i angrepene har økt betraktelig og således er vanskeligere å oppdage, på tross av at NSM har utviklet og forbedret sin evne til å detektere slike angrep (Nasjonal sikkerhetsmyndighet, 2015, s. 6). NSM beskriver utviklingen som et våpenkappløp, og at det er trusselaktørene som evner å utvikle seg raskere enn det NSM hadde mulighet til i 2015 (Nasjonal sikkerhetsmyndighet, 2015, s. 17). Dette er i tråd med Etterretningstjenestens vurdering, nemlig at det vil forekomme mer aggressive og målrettede forsøk på å trenge inn i datasystemer tilhørende norske styresmakter (Etterretningstjenesten, 2017, s. 34). Uavhengig av hvorvidt en øker evnen til deteksjon og håndtering av cyberangrep vil det alltid være en offensiv fordel ved at angriperen hurtig kan skifte mellom metoder og *veier* inn i systemet gjennom porter og sårbarheter, mens forsvareren må forsvare alle systemer og tilkoblingsmuligheter mot alle typer angrep samtidig (Lindsay, 2013, s. 376). Konklusjonen av disse faktorene blir et noe paranoid paradoks, nemlig at jo færre angrep som oppdages og håndteres, jo større kan trusselen være mot landets sikkerhet.

4.2.1 Delkonklusjon

Det er mange aktører som er interessert i å gjennomføre angrep mot Norge som stat og mot enkeltpersoner og bedrifter i Norge. Likevel utpeker det seg to stater som utgjør den største trusselen mot Norge i dag, nemlig Russland og Kina. De gjennomfører, og antas å fortsette å gjennomføre, etterretningsoperasjoner mot Norge i cyberspace. Selv om deres kapasiteter er ukjente kan de antas å besitte kapasiteter med stort skadepotensiale. Som NSM sier er det at antallet alvorlige hendelser de håndterer synker betyr ikke nødvendigvis at aktørenes innsats

avtar, men trolig at deres angrep blir mer sofistikerte og således vanskeligere å oppdage, hvilket bekreftes av Etterretningstjenestens vurdering.

4.3 Sårbarheter i Norge

> Sårbarhet betegner en begrenset evne til å tåle påkjenninger eller påvirkninger som kan resultere i betydelige negative avvik fra normal funksjon for det system som den sårbare komponent inngår i. Graden av sårbarhet beskriver hvor lett det er å påføre slik skade. (Forsvars- og justiskomiteen, 2002, s. 11)

Sårbarheter i IKT-systemer og EKOM-infrastruktur kan enten være tilstede som del av programvare eller komponenter, eller som del av en funksjon i systemet. Videre deles disse sårbarhetene inn i sårbarheter som er kjent, men aksepteres fordi det koster mer å utbedre enn det er verdt, og sårbarheter som er ukjent, feilvurdert, ikke forstått eller mangelfullt kommunisert (Norges offentlige utredninger, 2015, s. 31). Hvorvidt sårbarhetene som er kjent i samfunnet blir gjort noe med henger altså sammen med kostnaden av å utbedre sårbarheten sett opp mot skadepotensialet, risiko eller verdi av systemet som innehar sårbarheten.

Dagbladet hadde i 2013 en serie artikler der de undersøkte digital sårbarhet i Norge ved navn *Null CTRL*. I løpet av denne serien klarte journalistene ved hjelp av eksperter å søke opp over 2500 ulike ubeskyttede SCADA-systemer i Norge, hvorav 500 kontrollerte kommersiell eller samfunnskritisk infrastruktur (Hillestad, Sandli, & Strømman, 2013). Ifølge *Nasjonal strategi for informasjonssikkerhet (2012)* er det problematisk at flere av nevnte SCADA-systemer ikke lar seg oppgradere fordi de ikke kan kobles ut av drift, fordi ny programvare ikke er kompatibel med det gamle systemet, eller at det ikke eksisterer oppdateringer (Regjeringen, 2012, s. 5). Sårbarhetene som Dagbladet omtaler faller innunder kategorien av kjente sårbarheter som ikke anses til å være verdt å utbedre, hvilket betyr at de i utgangspunktet ikke ville utgjort stor skade på verken EKOM eller samfunnskritiske ressurser. Det er ikke heldig at slike sårbarheter eksisterer, men så lenge de er kjent vil det ikke kreve store ressurser for NSM eller andre sikkerhetsselskaper å overvåke systemet for å avdekke eventuelle angrep.

NATOs standpunkt for cyberforsvar er at hvert land er ansvarlig for sitt eget forsvar, selv om cyberangrep offisielt vil kunne utløse kollektivt forsvar i henhold til artikkel 5 (Wilson, 2016, s. 15) (NATO, 2014). Dette førere til at små land i utgangspunktet er mer sårbare enn de med omfattende forsvarsressurser (Wilson, 2016, s. 15). Som en av de mindre nasjonene i NATO

er Norge likevel i verdenstoppen når det gjelder bruk av IKT (Norges offentlige utredninger, 2015, s. 15). Denne kombinasjonen er urovekkende da det innebærer at vi, som en liten nasjon, er underlegne i møte med cyberstormakter og samtidig er helt avhengige av EKOM og IKT. Det er verdt å stille spørsmål ved hvorvidt vi må koble alt opp mot et nettverk. Kontreadmiral Nancy A. Norton sa i et intervju i 2016 at det første spørsmålet en bør stille seg angående nye systemer er hvorvidt en ønsker at det kobles til et nettverk, og om det er verdt de eventuelle konsekvensene (Taylor, 2016, s. 12). Dette er en avveining som bør foretas oftere enn det gjøres i samfunnet i dag. Norton utdyper: «Fixing the systems without addressing the people as part of it is worthless, because the people operating them is going to be the biggest vulnerability no matter what you do with the system» (Taylor, 2016, s. 13). Samtlige eksempler i denne oppgaven baserer seg i noen grad på en form for menneskelig svikt, noe som underbygger argumentet til Norman. Stuxnet-angrepet infiserte leverandører av programvare og komponenter til anlegget i Natanz, angrepet på strømnettet i Ukraina startet ved at ansatte åpnet Microsoft Office-dokumenter og industrispionasjesaken i Telenor startet ved at ledere enten måtte åpne og installere filer eller følge lenker i e-poster. IKT-systemer uten menneskelige brukere er ikke en realistisk løsning, men opplæring av det svakeste leddet i sikkerhetskjeden, nemlig mennesket, er både mulig og nødvendig.

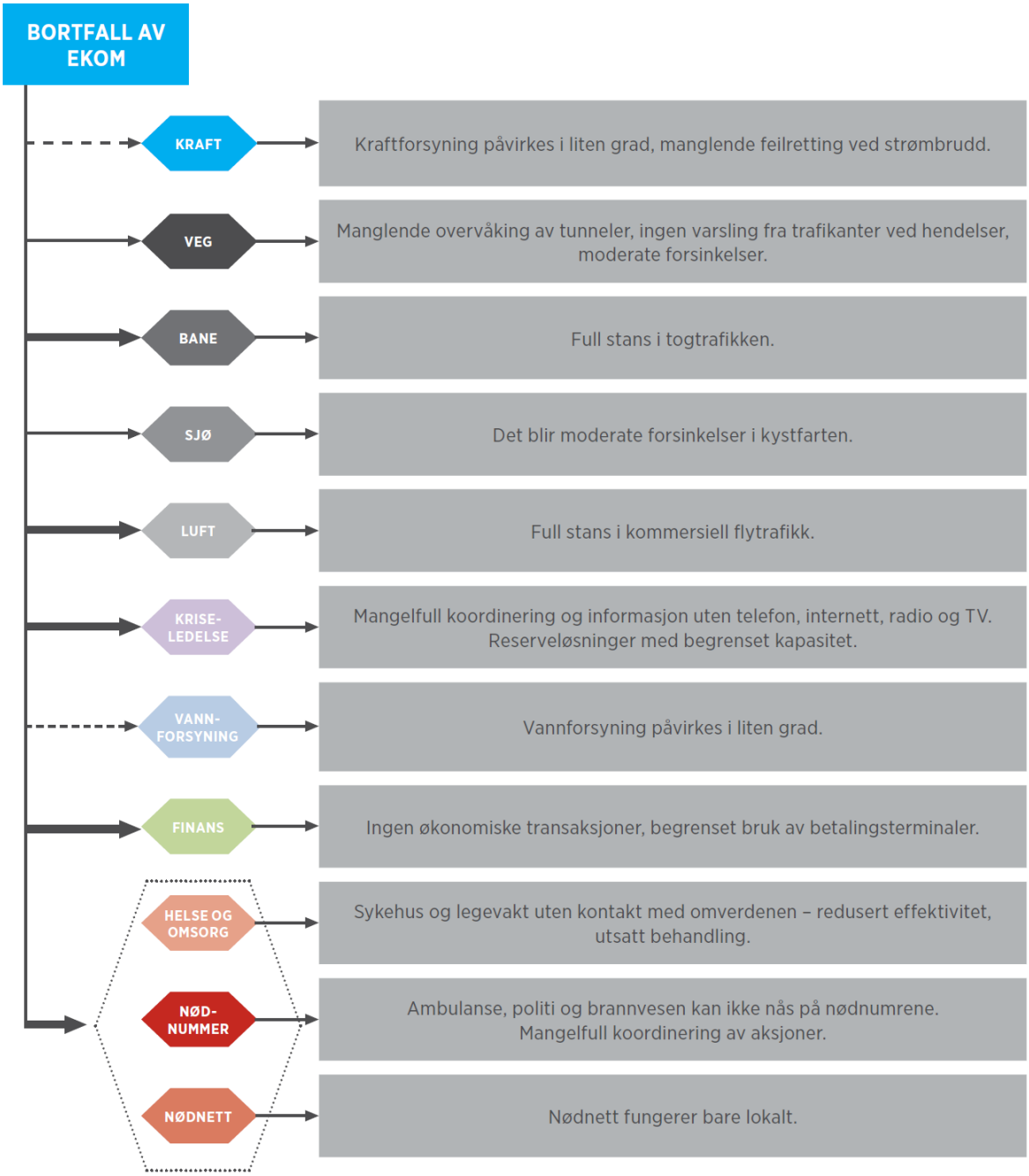
4.3.1 Delkonklusjon

Samfunnskritiske ressurser innehar i mange kjente sårbarheter som kan utnyttes av potensielle angripere. Stadig flere enheter og nettverk kobles ukritisk opp mot internett, en utvikling som kan antas å fortsette. Dette kan føre til at stadig nye sårbarheter etableres i Norge som kan by på utfordringer i morgendagens sikkerhetshverdag. Det er ukjente sårbarheter som byr på de største utfordringene for NSM i dag, og med utviklingen i samfunnet er det lite sannsynlig at det blir færre av disse i fremtiden. Det vil være hensiktsmessig å vurdere hvorvidt systemer må kobles opp mot internett for å bremse denne utviklingen.

4.4 Konsekvens

Konsekvens er en del av risikoen skissert tidligere i kapitlet. Risiko er sammensatt av to elementer, nemlig sannsynlighet og konsekvens (Norges offentlige utredninger, 2012, s. 68). «Konsekvensdelen, som er en vurdering av forventet negativ effekt, er i prinsipp lettere å kvantifisere og beregne, men beregningene blir ofte svært kompliserte» (Forsvars- og

justiskomiteen, 2002, s. 11). DSB gjennomførte i 2014 en analyse av konsekvensene av et cyberangrep mot EKOM-infrastruktur der scenariobeskrivelsen var at Telenors landsdekkende transportnett skades fysisk av et angrep på SCADA-systemene i tillegg til viktig programvare (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 12).



Figur 3: Hvilken grad kritiske samfunnsfunksjoner påvirkes av et EKOM-bortfall (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 37)

Som vist vil sektorene som rammes hardest være togtrafikk, flytrafikk, kriseledelse, finanssektoren og nødsentralene. Som analysen sier vil et så avansert cyberangrep bety at aktøren som står bak må være en statlig organisasjon, og at denne typen angrep trolig vil kombineres med andre typer angrep på landet (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 12). På bakgrunn av dette er det særdeles urovekkende at kriseledelse, nødsentralene og nødnettet er noen av de sektorene som blir hardest rammet og nærmest satt ut av funksjon i et nasjonalt perspektiv.

Forholdet mellom den virkelige verden og cyberspace er stadig i endring når samfunnet utvikler seg og blir mer avhengig av EKOM og IKT. Et rammeverk for å beskrive aktiviteter i cyberspace og den fysiske verden er å dele inn i fire områder: Cyber-cyber, cyber-fysisk, fysisk-fysisk og fysisk-cyber (Kuusisto & Kuusisto, 2015, s. 35). Disse beskriver veldig enkelt hvor angrepets opprinnelse finner sted, enten det er i cyberdomenet eller i den fysiske verden, og hvor konsekvensene av angrepet oppstår. Det er nødvendigvis angrep innen cyber-fysisk som umiddelbart vil utgjøre den største faren for skade på personer eller materiell. Kapasiteter som det Pentagon beskriver fjernstyre atomreaktorer til kjernenedsmelting hører hjemme i cyber-fysisk dimensjonen og vil utvilsomt være en omfattende konsekvens av cyberangrep, selv om dette per i dag ikke er noe en kan forvente (General Counsel of the Department of Defense, 2015, s. 1015). Angrep innen cyber-cyber dimensjonen kan likevel bety store konsekvenser for samfunnet, spesielt dersom en potensiell fiende fritt kan hente informasjon og etterretning fra systemer innen forsvar og beredskap (Etterretningstjenesten, 2017, s. 34). Konsekvensene av angrep, enten det er cyber-cyber eller cyber-fysisk, måles lettest i den fysiske verden ved hvor mange liv som kan gå tapt eller hvor mye materiell som ødelegges.

Thomas Rid argumenterer for at cyberangrep ikke vil resultere i direkte fysisk skade på mennesker, men at dette kun er en sekundær effekt av et eventuelt angrep (Rid, 2013, s. 12). Argumentet er at selve programkoden i et angrep ikke påfører skade, men at det eventuelt kan påføre skade ved å infisere et system og føre til at dette systemet påfører materiell eller personer skade (Rid, 2013, s. 13). Det er skadepotensialet til systemet under angrep som vil utgjøre den fysiske konsekvensen av et cyberangrep, noe som stemmer med hvordan *cyber fires* slik Pentagon beskriver de fungerer (General Counsel of the Department of Defense, 2015, s. 1015) (Rid, 2013, s. 13). Argumentet er absolutt gyldig, men en kan snu argumentet ved fysiske angrep. Dersom en bombe eksploderer i en tett bebygd by uten at noen dør av

eksplosjonen, har bomben ikke tatt livet av noen mennesker? Dersom det som følge av eksplosjonen bryter ut brann som tar livet av mennesker har disse menneskene omkommet som følge av bombeangrepet. På samme måte vil mennesker som omkommer av sekundæreffekter av cyberangrep være en konsekvens av selve cyberangrepet. Dette argumentet kan og trekkes langt, ved at en kan si at norske soldater som har tapt livet i Afghanistan omkom som følge av terrorangrepet 11. september som startet *krigen mot terror*.

4.4.1 Delkonklusjon

Konsekvensene av cyberangrep mot Norge kan være svært store. Vi vet ikke om det i dag er aktive spionasjeoperasjoner mot Norge som ikke er avdekket. Med bakgrunn i dagens situasjon kan en si det er stor sannsynlighet for at dette er tilfellet. Konsekvensene av at stormaktene innen cyberdomenet angriper Norge med det de besitter av kapasiteter vil trolig være svært omfattende. Det som er mest urovekkende er den pågående aktiviteten innen spionasje og utbygging av infrastruktur som allerede foregår, og at denne kan utnyttes ved fremtidige angrep (Etterretningstjenesten, 2017, s. 34). Sannsynligheten for et slikt angrep må ses i sammenheng med den ellers rådende sikkerhetspolitiske situasjonen i Norge, da det trolig ville kombineres med andre angrepsmidler. Dersom Norge skulle befinne seg i en konflikt som oppleves som en eksistensiell trussel for en av supermaktene innen cyberkrigføring vil vi se angrep som er langt med omfattende enn det vi hittil har sett (Limnéll, 2015, s. 529).

5 Konklusjon

Hensikten med denne studien er å besvare problemstillingen: **Er det en risiko for at Norge skal bli utsatt for et cyberangrep som får konsekvenser for landets sikkerhet?**

Risikoen for at vi blir utsatt for et slikt angrep vil være et resultat av hvilke aktører som har interesse av våre verdier, hvilken evne og vilje de har til å gjennomføre angrep, hvilke sårbarheter de kan benytte seg av for angrepet og til slutt hvilken konsekvens et gitt angrep vil få for landets sikkerhet. Det er ikke mulig å gi et konkret svar i form av en sannsynlighetsberegning for at noe slikt skulle inntreffe. Det vi med sikkerhet kan si er at potensialet for et slikt angrep absolutt er tilstede på bakgrunn av disse fire funnene:

1. Samfunnskritiske verdier er tilgjengelige for angrep via cyberspace dersom en potensiell aktør har interesse av det.
2. Blant de utpekte aktørene som gjennomfører angrep mot Norge er to av verdens stormakter innen cyberdomenet.
3. Det eksisterer både kjente og ukjente sårbarheter en angriper kan benytte seg av.
4. Konsekvensene av omfattende cyberangrep vil være av en slik art at de kan true landets og innbyggernes sikkerhet.

6 Bibliografi

1. Booz Allen Hamilton. (2016). *When the Lights Went Out - A Comprehensive Review of the 2015 Attacks on Ukranian Critical Infrastructure.* McLean: Booz Allen Hamilton Inc.
2. Clapper, J. R. (2016). *Worldwide Threat Assessment of the US Intelligence Community.* Senate Armed Service Committee.
3. Clausewitz, K. (2012). *On War*. Jersey City, USA: Start Publishing LLC.
4. Direktoratet for samfunnssikkerhet og beredskap. (2015). *Risikoanalyse av "Cyberangrep mot ekom-infrastruktur"*. Direktoratet for samfunnssikkerhet og beredskap.
5. E-ISAC SANS. (2016). *TLP: White - Analysis of the Cyber Attack on the Ukranian Power Grid.* Washington, D.C.: E-ISAC.
6. Enstad, K. (2016). Hvordan skrive en god tekst. Oslo, Oslo, Norge: Krigsskolen.
7. Etterretningstjenesten. (2017). *Fokus 2017.* Etterretningstjenesten.
8. Forsvars- og justiskomiteen. (2002). Innst. S. nr. 9. Oslo, Oslo, Norge: Forsvars- og justiskomiteen.
9. Forsvarsdepartementet. (2012, 03 23). Proposisjon 73 S. *Et forsvar for vår tid*. Oslo, Oslo, Norge: Regjeringen.
10. Forsvarsdepartementet. (2014, Mars 01). Forsvarsdepartementets retningslinjer for informasjonssikkerthet og cyberoperasjoner i forsvarssektoren. *FDs cyberretningslinjer*. Oslo, Oslo, Norge: Forsvarsdepartementet.
11. Forsvarsdepartementet. (2016). Proposisjon 151s - Kampkraft og bærekraft. Oslo, Oslo, Norge: Det kongelige forsvarsdepartement.
12. General Counsel of the Department of Defense. (2015, Juni). DoD Law of War Manual. Washington, D.C., Washington, D.C., USA: Department of Defense.
13. Gustavsen, I. H. (2015). *Når samfunnet lammes - militær bistand ved et dataangrep.* Oslo: Forsvarets stabsskole.
14. Hillestad, L. K., Sandli, E., & Strømman, O. (2013, Oktober 17). «I verste tilfelle kan liv gå tapt». *Dagbladet*.

15. International Telecommunication Union. (2017, Januar 12). *Statistics.* Hentet fra ITU: Committed to connecting the world: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
16. Johannesen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag AS.
17. Kuusisto, T., & Kuusisto, R. (2015). Cyber World as a Social System. I M. Lehto, & P. Neittaanmäki, *Cyber Security: Analytics, Technology and Automation* (ss. 31-43). Helsinki: Springer International Publishing.
18. Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal politikk*, ss. 229-240.
19. Langø, H.-I., & Sandvik, K. B. (2013, Juni). Cyberspace og sikkerhet. *Internasjonal politikk*, ss. 221-228.
20. Limnéll, J. (2015). The Exploitations of Cyber Domain as Part of Warfare: Russo-Ukranian war. *International Journal of Cyber-Security and Digital Forensics*, ss. 521-532.
21. Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, ss. 365-404.
22. Mærli, M. B. (2012). *Risikobasert sikring (security) og risikoreduksjon.* Oslo: Det Norske Veritas.
23. Nasjonal sikkerhetsmyndighet. (2015). *Årsrapport 2015.* Oslo: Nasjonal sikkerhetsmyndighet.
24. NATO. (2014, September 05). *NATO - Official text: Wales Summit Declaration*. Hentet fra NATO: http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber
25. NATO. (2016, Juli 09). *NATO - Official text: Warsaw Summit Communiqué*. Hentet fra NATO: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#top
26. Norges offentlige utredninger. (2006). *Når sikkerheten er viktigst - Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Oslo: Departementenes servicesenter Informasjonsforvaltning.
27. Norges offentlige utredninger. (2012). *Rapport fra 22. juli-kommisjonen.* Oslo: Departementenes servicesenter.
28. Norges offentlige utredninger. (2015). *Digital sårbarhet - sikkert samfunn.* Oslo: Departementenes sikkerhets- og serviceorganisasjon.
29. Regjeringen. (2012). *Nasjonal strategi for informasjonssikkerhet.* Oslo: Regjeringen.

30. Rid, T. (2013). *Cyber War Will Not Take Place.* London: Hurst & Company.
31. Samferdselsdepartementet. (2003, 07 25). Ekomloven. Oslo, Oslo, Norge: Stortinget.
32. Sternstein, A. (2015, November 15). The Secret Pentagon Push for Lethal Cyber Weapons. *Defense One*.
33. Store Norske Leiksikon. (2017, Februar 04). *Internett - Store norske leksikon*. Hentet fra SNL.no: https://snl.no/Internett
34. Taylor, D. P. (2016, April). Modern Cyber Warfare. *Sea Power Magazine*, ss. 12-13.
35. Wilson, J. R. (2016, Desember). The Shadowy World of Cyber Warfare. *Military & Aerospace Electronics*, ss. 8-15.